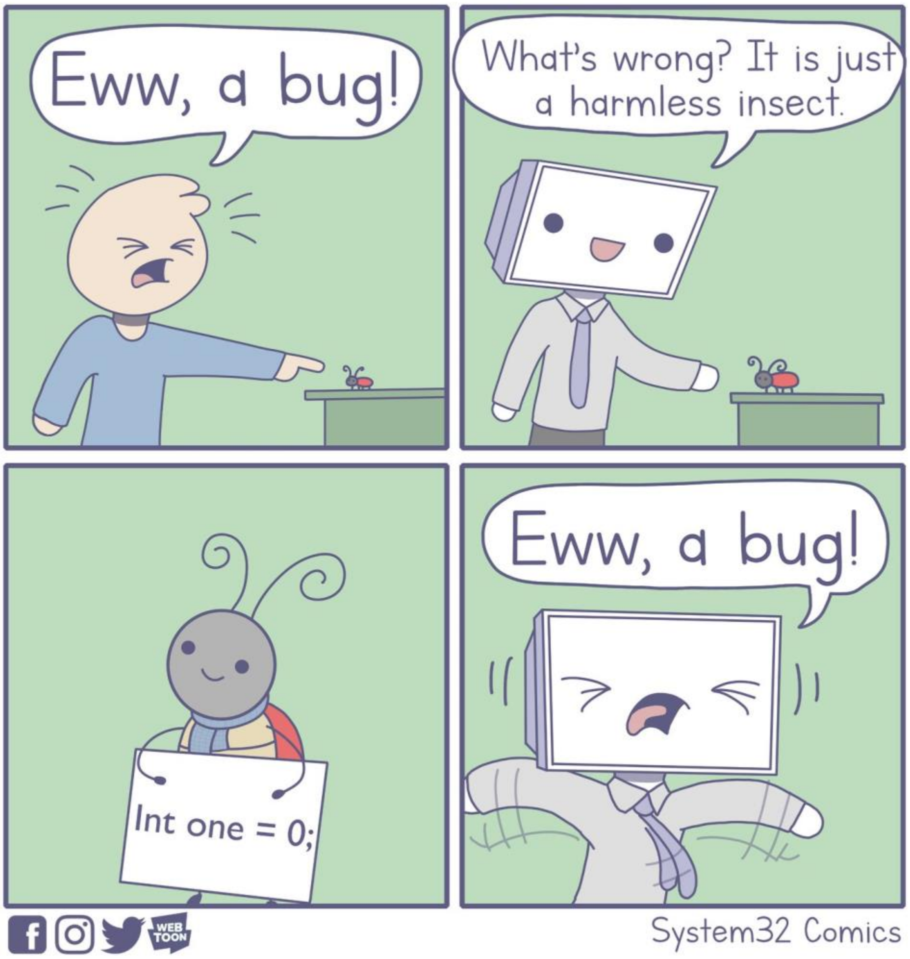

ASSIGNMENT 2

ITRI 625

ENRICO DREYER
31210783

Table of Contents

Introduction

In this assignment we were asked to identify a severe security threat to any aspect of NWU's IT infrastructure. I decided to focus on theft of data files and compile a security plan, business continuity plan and a risk analysis.

Security Plan

According to Blog (2010) a security plan is used to outline sensitive information that a company has, as well as the steps that the company take to ensure that the data stays safe. The issues that are going to be addressed are policy, current state, requirements, recommended controls, accountability, timetable, and maintenance.

Policy

Introduction

The "perfect" security does not exist, NWU strives to balance between the increasing level of security and the convenience of students and administrators.

Security responsibilities

- The website is hosted on a secure server environment.
- The links from the websites are under a control of third parties that are secure.
- Regular backups of all data.

Security disclaimers

- Third parties are responsible for security and information if they are used.
- We will ensure that any information is not compromised of our system.
- If any information is lost on your computer, we are not responsible for it.

Your security responsibilities

- Install external security on your own computer
- Run regular virus scans
- Update your security software

Protect your password

- Never share your password
- Never email your password
- Use a strong password

Current state

NWU is responsible for creating standards in their websites and web-applications. A risk analysis on the different vulnerabilities was done.

Threat	**Control in place**
Data breaches	Encryption
Unauthorized software	User Authorization
Bring your own device	User Accessibility

Requirements

Health Information and Privacy and Security Policy

The requirement is designed to ensure that NWU complies with all applicable state and federal laws, this includes individual's personal health and keeping the information of a person confidential and private.

Family Educational Rights and Privacy Act

This protects the confidentiality and privacy of student's educational records as well as give parents rights to respect their children's records.

Payment Card Industry (PCI) Data Security Standards

This is the standards and compliance to the requirements to protect a students payment card information. Additional regulations and laws apply for the search of unauthorized disclosure of individuals' information.

Data Protection requirements

Data is valuable to NWU, and some data should be protected with a higher level of security than others. The level is based on how important that data is, with confidentiality of students in mind. Physical security is also needed to keep data files safe and for confidential computing. This includes NWU making backups in the event of theft or loss to ensure that data is kept safe.

Recommended controls

- Apply antivirus solutions
- Implement perimeter defence
- Employee training and awareness
- Observe strict access controls

Accountability

The responsibility and authority that all departments of NWU and maintenance of authorization will keep data as safe as possible as well as monitoring the system.

Timetable

The plan is extensive, and security is never perfect. During the time, equipment will be upgraded and added. The plan is there to include growth and change as the security aspects changes. NWU experiences change in experience every day.

Maintenance

Threats in the environment are dynamic. With every maintenance, documentation is kept up to date with the current threat and security controls. Enforcement and monitoring is key to a success of the security controls, with monitoring the data at NWU easier maintenance can be done to ensure user data integrity. Maintenance includes updating the security plan to adapt to changing conditions(CDF, 2020).

Business continuity plan

According to Services (2020), a business continuity plan is there for a company to document the outlines of how a business will continue to work during an unplanned disruption in the working environment.

Business function recovery priorities

- Clear succession planning
- Reductions in resource availability
- Establish rules to triage requests
- Remote working capabilities
- Automation of standard tasks

Relocation strategy

NWU's workplace management has data capture and stores occupational data in central databases. Their data is stored in the cloud, making data migration easier. NWU also has recovery software to restore lost data efficiently and quickly. In terms of Natural disasters or workplace accidents NWU can implement:

- Remote working
- Relocation of offices or classes

Alternate business site

NWU uses an alternative business site in the event of a disruption or disaster to continue with business as usual. The short-term plan is to have students work from home (remote working) while the site is being renovated. The long-term plan is to rebuild the university for students to return to campus.

Recovery plan

With the plans in place to backup data in the cloud, NWU can recover data in an effective manner. In addition to the data stored on a computer, plans are in place to recover information that is stored op paper, this can include:

- Computer room environments
- Connectivity to service providers
- External hardware

Recovery phases

Disaster occurrence

NWU declares that a disaster occurred and decides if it is needed to proceed with the rest of the plan.

Plan Activation

NWU puts the business continuity plan in effect and will continue until the relocation of the campus is in operation and all the data is secured.

Alternate site operation

This phase is always in action until NWU can continue to its primary facility.

Transition to primary site

This phase is when NWU can continue to go back to the original site with all business operations.

Records backup

According to Secure_admin (2021), cloud backups are focused on copying files to locations that are remote from each other. NWU has hybrid backup, this mixes online backup and local backup. Hybrid backups allows NWU to recover data quickly as it runs transparently and in the background.

Restoration plan

Recovery teams controls, maintains, and check periodically on the records that are important to business operations. This affects the effectiveness of facility disasters and disruptions. The teams also backup and store critical files periodically to an offsite location.

Recovery Teams

NWU has established recovery teams and divide them into groups that are appropriate based on their title and job role.

Team roles

NWU has a team leader, Backup Leader, and team members.

Team Contracts

Depending on their roles, each member of the team has their own contract.

Team responsibilities

- HR/PR Officer
- Incident Commander
- Finance
- Admin
- Legal
- IT

Departmental recovery teams

- Emergency response team
- IT recovery team
- Human Resources team
- Business Continuity Coordinator

Recovery Procedures

1. Disaster Occurrence
2. Notify needed personnel
3. Plan activation
4. Relocate to alternative site
5. Establishment of communication
6. Alternative site operations
7. Transition back to primary operations
8. Relocate back to primary site if all is restored

Risk analysis

According to Hayes (2021) a risk analysis is a process of analysing the likelihood of an event occurring in a government, corporate or environmental sector. The study of risk analysis is the underlying unpredictability of a given event and the course of action, to forecast the probability of success or failure. Risk analysis enabled NWU to decide on what risk has the highest priority.

For NWU and the focus being theft of data files the following risk analysis was done:

Data Inventory

Type of data	Description	Level of sensitivity
Personal Information	Examples include Name, Address, CC number or social security number.	High
Financial Information	Examples include Credit card numbers, Expiry date, verification code, Transaction reference.	High

System Users

System Name	User Category	Access Level	Number of Users
Efundi	Students and Teachers	Read/Write	Everyone registered at NWU.
Nwu Site	Anyone	Read	Everyone

Threat Identification

Threat Source	Threat Action
Cyber criminal	• Identity theft • Social engineering • Web defacement
Employees	• Illness • Loss of key individuals
Technical	• System bugs • Failure of hardware • Malicious code
Environment	• Natural disasters • Man-made disasters
Organizational	• Reassignment actions • Work termination

Impact analysis

Incident	Consequence	Impact
Access to unauthorized information	• Loss of confidentiality • Loss of assets • Harm to organization	High
Unauthorized changes to system	• Loss of availability • Limited effect of operations • Unable to perform primary functions	Medium
Non-sensitive data being lost	• Loss of integrity • Limited assets or individuals • Can perform primary functions	Low

Risk analysis result

Threat	Vulnerability	Mitigation	Likelihood	Impact	Risk
Natural disaster	Power outage, loss of working site	Generators and alternative sites	Moderate to low	Medium	High
Lack of recovery plan	Disaster recovery	Develop a recovery plan	Moderate	High	Moderate
Unauthorized user access	Access to sensitive data	System security monitoring, testing, and securing system	Moderate	High	Moderate

Conclusion

In this assignment we were asked to identify a severe security threat to any aspect of NWU's IT infrastructure. I decided to focus on theft of data files and compiled a security plan, business continuity plan and a risk analysis.

References

Blog, S. X. (2010). How to create an Information Security Plan. https://myshugo.wordpress.com/2010/05/09/how-to-create-an-information-security-plan/#:~:text=An%20information%20security%20plan%20is%20a%20document%20that,response%20in%20the%20event%20of%20a%20data%20breach.

CDF. (2020). Security Plan Guidance. https://www.cdc.gov/selectagent/resources/Security_Plan_Guidance.pdf

Hayes, A. (2021). Risk Analysis. https://www.investopedia.com/terms/r/risk-analysis.asp

Secure_admin. (2021). All you need to know about disaster recovery and backup (BDR). https://manageditservicescharleston.com/all-you-need-to-know-about-disaster-recovery-and-backup-bdr/

Services, I. (2020). What is a business continuity plan? https://www.ibm.com/services/business-continuity/plan